78-1228

No.

IN THE

Supreme Court of the United States

OCTOBER TERM, 1978

BERTRAM E. SEIDLITZ,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

DAVID M. DORSEN
SACHS, GREENEBAUM & TAYLER
1620 Eye Street, N.W.
Washington, D.C. 20006
Attorneys for Petitioner

THE CASILLAS PRESS, INC.—1717 K Street, N. W.—Washington, D. C.—223-1220

TABLE OF CONTENTS

TABLE OF AUTHORITIES

IN THE

Supreme Court of the United States

OCTOBER TERM, 1978

No.

BERTRAM E. SEIDLITZ,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

Petitioner prays this Court to issue a Writ of Certiorari to review the Judgment and Opinion of the United States Court of Appeals for the Fourth Circuit.

DECISION BELOW

The Judgment and Opinion of the United States Court of Appeals for the Fourth Circuit in *United States v. Bertram E. Seidlitz*, No. 76-2027 (4th Cir. Dec. 5, 1978), has not yet been officially reported. A copy of that Judgment and Opinion is appended hereto.

JURISDICTION

Jurisdiction is invoked under Title 28, United States Code, Section 1254(1), and the Fourth Amendment to the United States Constitution. Judgment was entered by the Court of Appeals on December 5, 1978. A timely petition for rehearing was filed but denied on January 9, 1979.

QUESTIONS PRESENTED

1. Must the provisions of the Fourth Amendment to the United States Constitution be complied with when the Federal Bureau of Investigation requests a private party to conduct a search, the private party conducts it because of the request, and the fruits of the search are immediately turned over to the FBI and utilized in a search warrant as well as introduced in evidence at trial?

2. Does the installation of a telephone tracing device on a person's telephone in the above circumstances without a court order or search warrant violate the Fourth Amendment to the United States Constitution?

CONSTITUTIONAL PROVISION INVOLVED

AMENDMENT IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

STATEMENT OF THE CASE

Petitioner was tried and convicted of two counts of fraud by wire in violation of 18 U.S.C. § 1343. Prior to trial, petitioner filed a motion to suppress certain evidence, including the evidence that forms the basis for this Petition, on the ground, *inter alia*, that it was obtained in violation of the Fourth Amendment. The trial court denied the motion. Following a six-day trial before the court and a jury, petitioner was convicted and sentenced to serve three months in custody as well as a period of probation.

The facts are as follows:

On January 1, 1975, petitioner was employed as a computer specialist and project director with Optimum Systems, Inc. (OSI) in connection with a project to install, maintain and operate a computer facility for use by the Federal Energy Administration (FEA). When completed, persons working for FEA in various parts of the country could communicate with the OSI facility, located in Rockville, Maryland, over telephone wires. In June 1975, petitioner resigned his position and returned to work at his own computer firm in Alexandria, Virginia.

In late December 1975, FEA and OSI employees, in an effort to see who was using the OSI system, observed that an unauthorized person had gained access to the computer. The employees determined that the computer was transmitting to the unauthorized person a portion of a "source code" for the system, programming language that is used to give instructions to the computer. They also ascertained that the data was being transmitted outside the OSI facility. At the employees' request, the telephone company twice manually traced calls, without listening to their content, to the Alexandria, Virginia, office of petitioner's company.

The FBI was then contacted. At the FBI's request, the telephone company conducted two additional manual traces, but in each instance the calls were terminated before the traces had progressed beyond the telephone company's office in Lanham, Maryland, which served 10,000 subscribers. The telephone company then installed "original

accounting identification equipment" in the Lanham office, which would automatically ascertain, without hearing the content of the call, the telephone number of any of the 10,000 telephones from which calls to OSI were being made.

Two such calls were made to OSI on the morning of January 9, 1976, both of which were traced to petitioner's residence in Lanham, Maryland, which, like Rockville, where OSI's facility was located, is a Maryland suburb of Washington, D.C. On the same day, relying on these traces, the FBI secured and executed a search warrant on petitioner's residence, as well as a search warrant for the premises of petitioner's computer company, which it had obtained on January 3, 1976. The execution of the search warrants produced incriminating evidence.

In an oral opinion, the trial judge denied petitioner's motion to suppress, including the portion relating to the January 9, 1976, traces, on the ground that neither the Fourth Amendment nor Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 ff., were violated since no "interception" took place. Over objection, the results of the January 9, 1976, traces as well as evidence seized at petitioner's residence were introduced at trial.

The Court of Appeals affirmed. In its opinion the Court of Appeals concluded that following the telephone traces that led to petitioner's computer company, "[a]t the FBI's suggestion" the telephone company conducted two additional manual traces which led to its Lanham, Maryland, office and then proceeded to install the automatic tracing equipment, which identified petitioner's residence as the source of the calls (Appendix A-5). The Court's conclusion as to the FBI's role is fully supported by the record. The testimony at the suppression hearing on the subject was provided by a telephone company security supervisor, who testified under questioning by government counsel:

Q. Now, as a result of the two incomplete traces on January 5, 1976, what, if anything, did you do?

A. Because I was informed by Phil Muello, Special Agent, FBI, that it was an on going investigation and requested Telephone Company's cooperation to ascertain any future calls to the Optimum Systems, calls in question on demand, and because we had a local area location in Lanham, on the 6th of January, preceding [sic] the traces on the 5th, I placed an automatic test in the Lanham office. . . .

In its opinion, the Court of Appeals nevertheless stated:

> The last of the objections raised in the court below to the evidence secured by Milten Spy and the telephone traces was that it was detected and obtained in contravention of the Fourth Amendment. The district judge rejected this contention on the ground that even though the "spy" and the traces were utilized without prior judicial authorization, the evidence was obtained by searches to which the appropriate persons had consented. We need not review the soundness of that ruling or the implicit conclusion that the "spy" and the traces raised questions under the Fourth Amendment, since in our opinion the activities complained of were, at most, conducted by private persons — OSI and the telephone company — to which the constitutional prohibition against warrantless searches does not apply. [Appendix A-2.] [Footnote omitted.][1]

The Court of Appeals affirmed petitioner's conviction and denied his petition for rehearing.

[1] In the omitted footnote (numbered 20) the Court of Appeals stated that "the parties have not briefed" the applicability of the Fourth Amendment to the telephone traces. That statement is incorrect. By

REASONS FOR GRANTING WRIT

In sum, there are two Questions Presented, each of which merits consideration by this Court. First, the decision of the Court of Appeals that compliance with the provisions of the Fourth Amendment was not required is inconsistent with a decision of this Court, decisions of other Courts of Appeals and a decision of the Court of Appeals of the State of Maryland in a case in which this Court has granted a petition for *certiorari*. *Michael Lee Smith v. Maryland*, 283 Md. 156, 389 A.2d 858 (1978), *cert. granted*, 47 U.S.L. Week 3391 (No. 78-5374, December 4, 1978). Second, this case raises an issue, namely, whether the installation of a tracing device on a person's telephone without a court order or search warrant violates the Fourth Amendment, on which this Court has granted *certiorari* in *Smith v. Maryland, supra.*

A. Contrary to Decisions of This Court and Courts of Appeals, the Fourth Circuit Erroneously Held That the Tracing of Petitioner's Telephone Calls Involved No Governmental Action.

In connection with its investigation into fraud by wire, 18 U.S.C. §1343, the Federal Bureau of Investigation requested the telephone company to ascertain who was making interstate telephone calls to OSI (Appendix A-5).

leave of court, and prior to oral argument, petitioner filed a Supplemental Brief, whose only point related to the January 9, 1976, traces. Indeed, the only argument heading in that brief reads: "The Telephone Company Acted Unlawfully in Tracing Telephone Calls of Mr. Seidlitz." The telephone company employee's testimony quoted above appears in the Supplemental Brief and virtually all the cases discussed below are cited therein. The Petition for Rehearing filed in the Court of Appeals dealt solely with the January 9, 1976, traces.

The Milten Spy referred to in the opinion was an internal monitoring system of OSI and indicated the content of what was being transmitted.

Because of that request, the telephone company put a tracing device on petitioner's home telephone, along with the telephones of approximately 10,000 other subscribers. On January 9, 1976, the tracing device identified petitioner's home telephone as the one originating the call to OSI. Also on January 9, that information was supplied to the FBI, which incorporated it into an application for a search warrant and obtained and executed upon that warrant. Nevertheless, the Court of Appeals held that the actions complained of were "conducted by private parties" (Appendix A-12).

Thirty years ago, in *Lustig v. United States*, 338 U.S. 74, 78-79 (1949), this Court articulated the test that has been applied ever since to determine whether there was governmental versus private action under the Fourth Amendment:

> The crux of that doctrine is that a search is a search by a Federal official if he had a hand in it. . . . The decisive factor in determining the applicability of the *Byars* case is the actuality of a share by a fed :al official in the total enterprise of securing and selecting evidence by other than sanctioned means. It is immaterial whether a federal agent originated the idea or joined in it while the search was in progress. So long as he was in it before the object of the search was completely accomplished, he must be deemed to have participated in it.

In the present case, the federal government had a major share in the search — the search was requested by the FBI, the search was conducted because of the FBI's request, the search was conducted to further the FBI's investigation and the results of the search were promptly turned over and used by the FBI. In fact, unlike in *Lustig*, the FBI "was the moving force of the search," a circumstance which this Court assumed would make the search federal action.

Courts that have faced the question of whether a search is federal action when it is motivated by federal officials and conducted for federal law enforcement purposes have uniformly answered the question in the affirmative. *Corngold v. United States*, 367 F.2d 1, 5 (9th Cir. 1966); *United States v. West*, 453 F.2d 1351, 1356 (3d Cir. 1972); *United States v. Ford*, 525 F.2d 1308, 1312 (10th Cir. 1975); *see United States v. Crabtree*, 545 F.2d 884 (4th Cir. 1976). Furthermore, in a case in which this Court has granted a writ of *certiorari* to the Court of Appeals of Maryland, this Court's jurisdiction is based upon the circumstance that police officers requested a private person to do an act in furtherance of their investigation. *Smith v. Maryland, supra*, 389 A.2d at 859-60.

B. The Tracing of Telephone Calls From Petitioner's Residence Violated His Fourth Amendment Rights.

In *Smith v. Maryland, supra*, this Court has granted *certiorari* on the precise question on which petitioner seeks review. Thus, *certiorari* is pending in order to decide whether it is violative of the Fourth Amendment for the government to place tracing devices on a suspect's telephone without securing a search warrant or court order. As the petition for *certiorari* in that case correctly points out, the clear weight of authority is contrary to the decision in that case, which was that no constitutional rights of the defendant were violated. *See United States v. Giordano*, 416 U.S. 505, 548, 553-54 (1974) (Powell, J., concurring); *Application for an Order Authorizing the Use of a Pen Register or Similar Mechanical Device*, 538 F.2d 956 (2d Cir. 1976) *aff'd in part on other grounds sub nom.; United States v. New York Tel. Co.*, 434 U.S. 159 (1977); *United States v. Illinois Bell Tel. Co.*, 531 F.2d 809 (7th Cir. 1976); *Application of the United States for an Order Authorizing Installation and Use of Pen Register*, 546 F.2d 243 (8th Cir. 1976), *cert. denied*, 434 U.S. 1008 (1978); *United States v. Lanza*, 341 F.Supp. 405 (M.D. Fla. 1972); *but see United States v. Clegg*, 509 F.2d 605, 610 (5th Cir. 1975).

In the present case, the telephone company, at the instigation of the FBI, did just what the telephone company did in *Smith v. Maryland*, namely, place a device on the suspect's end of the telephone transmission in order to see who was placing calls to the victim of a crime. The Court of Appeals in the present case, however, concluded that no governmental action was involved and it therefore did not have to decide "the 'open' question of whether the Fourth Amendment applies to such traces." (Appendix A-12 n.20). Since the Court of Appeals was in error on the issue of whether there was governmental action and this Court has agreed to decide the question of whether a search warrant or other court order is required to install a tracing device in these circumstances, there is compelling reason for this Court to grant *certiorari* herein as well.

CONCLUSION

For the reasons heretofore cited it is respectfully submitted that a writ of *certiorari* to the United States Court of Appeals for the Fourth Circuit be issued herein.

David M. Dorsen
Attorney for Petitioner

APPENDIX A

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

No. 76-2027

UNITED STATES OF AMERICA,

Appellee,

versus

BERTRAM E. SEIDLITZ,

Appellant.

Appeal from the United States District Court for the District of Maryland, at Baltimore. Alexander Harvey, II, District Judge.

Argued July 19, 1978 Decided December 5, 1978

Before WINTER, Circuit Judge, FIELD, Senior Circuit Judge, and HALL, Circuit Judge.

David M. Dorsen (Sachs, Greenebaum & Tayler; Beverly Sherman Nash, Sachs & Greenebaum on brief) for Appellant; Robert A. Rohrbaugh, Assistant United States Attorney (Russell T. Baker, Jr., United States Attorney on brief) for Appellee.

FIELD, Senior Circuit Judge:

Bertram Seidlitz appeals from his conviction on two counts of fraud by wire in violation of 18 U.S.C. § 1343.[1] As grounds for reversal, he urges that the trial court erred in its denial of a pretrial motion to suppress evidence, and that the prosecution failed to establish certain material elements of the crime. Although advanced in a somewhat novel factual context, we find appellant's contentions to be without merit.

On January 1, 1975, defendant Seidlitz assumed the position of Deputy Project Director for Optimum Systems, Inc. (OSI), a computer service company which was under contract to install, maintain, and operate a computer facility at Rockville, Maryland, for use by the Federal Energy Administration (FEA). Under the arrangement between OSI and FEA, persons working for FEA in various parts of the country could use keyboards at communications terminals in their offices to send instructions over telephone circuits to the large computers in Rockville, and the computers' responses would be returned and reflected on a CRT (cathode ray tube) terminal which is a typewriter-like device with a keyboard and display screen similar to a television screen upon which the information is displayed as it is sent and received.[2] Mr. Seidlitz helped to

[1]The federal wire fraud statute, 18 U.S.C. § 1343, provides:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined not more than $1,000 or imprisoned not more than five years, or both.

[2]A remote user would dial on an ordinary telephone one of the several unpublished telephone numbers to which OSI subscribed and which were assigned to the computers. He would then connect the telephone to his terminal so that messages could be relayed between the terminal and the computers in the form of signals traveling over the telephone line. Because any of a number of commercially available terminal units could accomplish such a link to the computers, the user, as a security precaution, had to enter on his terminal keyboard a special access code before he would be permitted full use of the system. The code contained, among other things, the user's personal initials, which were to be invalidated when he left OSI or FEA. This "access code" would be communicated to the central computers which, if they recognized the code as belonging to an authorized user, would proceed to perform the work the individual sent along.

prepare the software[3] which was installed at the Rockville facility as part of the project, and he was also responsible for the security of the central computer system. During his tenure, he had full access to the computers and to a software system known as "WYLBUR" which resided within them.[4] In June, 1975, Seidlitz resigned this job and returned to work at his own computer firm in Alexandria, Virginia.

William Coakley, a computer specialist employed by FEA, was assigned temporarily to the OSI facility. On December 30, 1975, in an attempt to locate a friend who might be using the OSI system, he had the computer display the initials of everyone who was then using the WYLBUR software. Among the initials displayed by the computer were those of his supervisor, who was standing nearby and who was not using the computer. Suspicious

[3]To be distinguished from "hardware," which is the tangible machinery of the computer, "softwear" refers to the logic and directions loaded into the machine that cause it to do certain things on command.

[4]The WYLBUR software system facilitated the computers' exchanges with FEA users at the remote terminals. It contained no classified FEA information, but rather enabled the computers to perform tasks assigned to them by FEA personnel. An OSI manual described WYLBUR as "an online interactive text editor designed to facilitate the creation of text and to provide a powerful and comfortable tool for changing, correcting, searching and displaying text."

that an unauthorized "intruder" might be using these initials in order to gain access to the system,[5] Coakley asked Mr. Ewing, an OSI employee, if Ewing could determine what was happening. He also asked Mr. Wack, an OSI supervisor, if he (Wack) could determine whether the mysterious user was at a remote terminal or at one of the terminals within the OSI complex which were directly wired to the computer and did not employ telephone circuits. Ewing instructed the computer to display for him the data it was about to transmit to the possible intruder, and it proved to be a portion of the "source code" of the WYLBUR software system.[6] Using other data provided by the computer, Wack concluded that the connection was by telephone from outside the complex. At his request, the telephone company manually traced the call to the Alexandria office of the defendant.[7] Wack was told that the trace was successful, but the telephone company informed him that it could not divulge the results of the trace except in response to a legal subpoena.

The following day, OSI activated a special feature of the WYLBUR system known as the "Milten Spy Function," which automatically recorded, after they had been received by the machinery at Rockville, any requests made of the computer by the intruder. The "spy" also recorded, before they were sent out to the intruder over the telephone lines, the computer's responses to such requests. Mr. Wack again asked the telephone company to trace the line when it was suspected that the unauthorized person, employing the same initials, was using the computer to receive portions of

[5] *See* n. 2, *supra.*

[6] A source code is a programming language, understandable to humans, in which a computer is given instructions.

[7] A manual trace is accomplished without listening in on the line or breaking into the conversation. It entails a physical tracing of the telephone circuitry backward through the various switching points from the equipment which receives the call.

the WYLBUR source code. This manual trace on December 31 led once more to the defendant's office in Virginia, although OSI was not so informed.

Advised by OSI of the events of December 30 and 31, the FBI on January 3, 1976, secured, but did not then execute, a warrant to search the defendant's Alexandria office.[8] At the FBI's suggestion, the telephone company conducted two additional manual traces when alerted to incoming calls by OSI, but in each instance the calls were terminated before the traces had progressed beyond the telephone company's office in Lanham, Maryland, which served 10,000 area telephones from which any subsequent calls to "originating accounting identification equipment" in the Lanham office, the function of which was to automatically and quickly ascertain, without intercepting the contents of any communication, the telephone number of any of the 10,000 area telephone from which any subsequent calls to the OSI computers originated. Two such calls were made on the morning of January 9, and the equipment attributed both of them to a phone at the defendant's Lanham residence. That afternoon, the FBI executed the warrant to search Seidlitz' Alexandria office, seizing, among other items, a copy of the user's guide to the OSI system and some 40 rolls of computer paper upon which were printed the WYLBUR source code.[9] A warrant was then issued to

[8] The affidavit in support of the application for the warrant related that the intrusions had been detected, that OSI had "furnished written release" to receive information regarding the telephone traces of December 30 and 31, and that the telephone company had disclosed to the FBI that the calls originated from the defendant's office. It also stated that, as a result of an investigation of former OSI employees and interviews with OSI personnel, the FBI, prior to the receipt of the trace information, had ascertained Seidlitz' business address and concluded that he was the chief suspect.

[9] The information on these printouts was identified at trial as being identical to the information recorded by the "spy" program on December 31.

search the Seidlitz residence in Lanham,[10] where officers found a portable communications terminal which contained a teleprinter for receiving written messages from the computer, as well as a notebook containing information relating to access codes[11] previously assigned to authorized users of the OSI computers.

The indictment handed down on February 3, 1976, charged that the defendant had, on December 30 and 31, transmitted telephone calls in interstate commerce as part of a scheme to defraud OSI of property consisting of information from the computer system.[12] A motion to suppress the evidence seized from the office and the residence was considered at a hearing on April 30,[13] after which the district judge rendered an oral opinion rejecting the defendant's argument that the searches were invalidated by the use of illegal electronic surveillance to obtain the information contained in the affidavits supporting the warrants. Specifically, the district judge ruled that (1) as to the information obtained by use of the "spy", Section 605 of the Communications Act of 1934, 47 U.S.C. § 605, does not apply, and neither Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510, *et seq.*, nor the Fourth Amendment were violated, since the information was obtained with the consent of a party to the defendant's telephonic communications, and (2) with

[10]The affidavit in support of the application for this warrant in essence contained the same statements made in the application for the prior warrant. *See* n. 8, *supra*. In addition, it related that the FBI had been informed that Seidlitz maintained a communications terminal at his home, that the search of the office had not uncovered the terminal, and that the telephone company's trace of the calls that morning indicated that they were made from the defendant's residence.

[11]*See* n. 2, *supra*.

[12]A motion for acquittal on a third count of interstate transportation of stolen property was granted during the course of the trial.

[13]The evidence presented at the suppression hearing established all the facts which we have summarized above.

respect to the tracing of the telephone calls, neither Title III nor the Fourth Amendment are offended when, as in the "pen register" cases, the number of the telephone from which a call is placed is determined by a process which does not entail the interception of the contents of the communication. Over defense objection, much of the challenged evidence was admitted at trial, and the telephone traces, as well as the operation of the "Milten Spy", were described to the jury. In the face of this evidence, the defendant conceded that he had retrieved the information from the computers, but claimed to have acted only out of concern for the security of the OSI system. In negation of fraudulent intent, Seidlitz testified that he acquired the data with the sole intention of presenting the printouts to OSI officials to prove to them that the steps taken to prevent unauthorized use of the computers were inadequate. Additionally, it was his position at trial that the WYLBUR software was not a trade secret or other property interest of OSI sufficient to qualify as "property" within the meaning of the wire fraud statute. On appeal he renews the "illegal surveillance" claims and also argues that the evidence before the jury was insufficient to establish either his fraudulent intent or that WYLBUR constituted "property."

In considering the surveillance questions, we assume that if, as the defendant contends, either the "spy" activities or the traces were conducted illegally, then the evidence seized at both the office and the residence should have been suppressed, since the affidavits upon which the warrants were issued contained information attributable to the "spy" and the telephone traces which was essential to the finding of probable cause to search.[14] Furthermore, if the statutory or

[14]In ruling on the motion to suppress, the district court also made this assumption. "[T]he question is whether the information * * * was legally or illegally secured. If, of course, it was illegal, then the searches must fail. * * *". Appendix, p. 133.

constitutional standards upon which the defendant relies were transgressed, then the jury should not have been informed of the deployment of the "spy" and the traces of the telephone calls.[15]

It can safely be said, however, that even if, as the defendant argues, the Milten Spy or the telephone traces resulted in the "interception" of his communications with the computers, these communications were wire or telephone communications since in each instance the defendant was exchanging messages with the computers over commercial telephone circuits.[16] For this reason the district court correctly concluded that Section 605 of the Communications Act of 1934, 47 U.S.C. § 605, could have no bearing whatever upon the legality of these activities. While at one time Section 605 did contain standards for determining the legality of the interception of telephone conversations, the statute was amended by Section 803 of Pub. L. 90-351, 82 Stat. 223, in 1968, for the express purpose of excluding from its scope the interception of wire communications and of transferring the regulation of such activity to certain provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968. *See United States v. Clegg*, 509 F.2d 605, 611-612 (5 Cir. 1975); *United States v. Falcone*, 505 F.2d 478, 482 (3 Cir. 1974), *cert. denied* 420 U.S. 955 (1975); S. Rep. No. 1097, 90th Cong., 2d Sess. 107 (1968), *reprinted in* [1968] U.S. CODE CONG.

[15]Section 605 of the Communications Act has been interpreted to require the exclusion of evidence obtained in violation thereof, *Nardone v. United States*, 302 U.S. 379 (1937), and an express exclusionary rule is contained in Title III of the Omnibus Act at 18 U.S.C. § 2515. A judicially-fashioned rule of exclusion applies where surveillance does not comport with Fourth Amendment requirements. *Katz v. United States*, 389 U.S. 347 (1967).

[16]The same can be said of Mr. Ewing's inquiry of the computer on December 30 by which he ascertained, as did the Milten Spy on the following day, that the intruder was receiving part of the WYLBUR source code.

& AD. NEWS 2112, 2196. Today Section 605 pertains to the interception of only radio communications, and there is no indication that radio communications of any kind were involved in the apprehension and conviction of the defendant. The appropriate inquiry, then, is whether any of the questioned activities amounted to the kind of interceptions of wire communications condemned by Title III.

The language, the legislative history, and the Supreme Court's interpretation of the relevant provisions of Title III support the district court's conclusion that the telephone traces in this case were not the sort of "interceptions" of communications proscribed by the statute. "Intercept" is defined in 18 U.S.C. § 2510 (4) to mean "the aural acquisition of the *contents* of any wire or oral communication through the use of any electronic, mechanical, or other device" (emphasis added); "'contents' * * * includes any information concerning the identity of the parties to [the] communication or the existence, substance, purport, or meaning of [the] communication." 18 U.S.C. § 2510 (8). The evidence adduced at the suppression hearing conclusively shows that neither the manual traces conducted on December 30 and 31, nor the traces which were achieved by use of the special equipment later installed, entailed interference with or observation of the contents of the defendant's dialogues with the computers. That Congress intended to exempt such procedures from the coverage of the statute is borne out by the Senate Report which accompanied the legislation, and explained that

> "[t]he proposed legislation is not designed to prevent the tracing of phone calls * * *. The proposed legislation is intended to protect the privacy of the communication itself and not the means of communication."

S. Rep. No. 1097, *supra*, at 90; U.S. CODE CONG. & AD. NEWS, *supra*, at 2178. *See Michigan Bell Tel. Co. v. United States*, 565 F.2d 385, 387-389 (6 Cir. 1977). Especially in view of *United States v. New York Telephone*

Co., 434 U.S. 159 (1977), which held that "pen registers" (which similarly "overhear" none of the substance of a telephone communication, 434 U.S. at 161, n.1) do not run afoul of the statute, we perceive no reason to invalidate the telephone traces on statutory grounds.

We also concur in the disposition by the court below of the challenge under Title III to the information obtained through the use of the Milten Spy. First, the statute proscribes only the "aural" acquisition of the contents of wire communications, 18 U.S.C. § 2510 (4), *supra*, and there is no evidence to suggest that the "spy" relied in any fashion upon sounds in retrieving information from the computers in written form. *Cf. United States v. New York Telephone Co, supra*, 434 U.S. at 166-167. We find no merit in the defendant's suggestion that, in the absence of either a statutory definition of the word "aural" or of legislative history to indicate that Congress even considered the relationship of Title III to computer systems, we should ignore the plain meaning of the term "aural"[17] and should hold that, regardless of whether a device detects sound, its ability to interpret the substance of a transmission brings it within the restrictions of the statute. Canons of statutory construction require that we attribute to legislatively undefined words their commonly accepted meaning and that we give effect to what must be presumed to have been the purposeful inclusion in the legislation of a qualifying term such as "aural" which restricts the statute's scope.[18] Second, to the extent that the Milten Spy disclosed, *before* they were sent out over the telephone lines, the substance of

[17] "The words 'aural acquisition' literally translated mean to come into possession through the sense of hearing (Webster's Third New International Dictionary, 1967 Ed.)." *Smith v. Wunker*, 356 F.Supp. 44, 46 (S.D. Ohio 1972).

[18] *See Platt v. Union Pacific R.R. Co.*, 99 U.S. 48, 58-59 (1878); *State Water Control Board v. Train*, 559 F.2d 921, 914 n. 20 (4 Cir. 1977). These rules are applicable here because the legislative history indicates neither what Congress meant by "aural" nor why the word was written into the statute.

the replies generated by the computer to the intruder's commands, the information was not a "wire communication" at the time of its retrieval, and its disclosure thus did not violate the statute. Under Title III, a "wire communication" is a communication made "in whole or in part" through the facilities of a common carrier, 18 U.S.C. § 2510 (1), and the portion of the WYLBUR source code requested by Seidlitz was obtained by the "spy" before it had travelled through such facilities. While arguably this reasoning might not apply to the spy's duplication, after they had been received by the computer, of any of the instructions Seidlitz sent by telephone, it unquestionably legitimizes under the statute that portion of the retrievals which identified the outgoing information as the WYLBUR source code. Finally, Title III specifically authorizes the interception of a wire communication by a party to the communication or by a person acting with the consent of a party to the communication. 18 U.S.C. § 2511 (2) (c), (d). In our opinion OSI, which leased, housed, programmed, and maintained the computers and subscribed to the relevant telephone numbers, was for all intents and purposes a party to the communications initiated by the defendant, since in a very real sense the company used the computers solely as a medium for imparting to customers, via telephone lines, its own expertise. Insofar as OSI installed on its line a computer which was capable of recording the messages exchanged in the course of responding to a remote user's requests, we consider this case analogous to those which recognize that a party may, consistent with Title III, use a device to capture and record both sides of his telephone conversation with another party. *See, e.g., United States v. Turk*, 526 F.2d 654 (5 Cir. 1976), *cert. denied*, 429 U.S. 823 (1976); *Smith v. Cincinnati Post & Times-Star*, 475 F.2d 740 (6 Cir. 1973); *Smith v. Wunker*, 356 F.Supp. 44 (S.D. Ohio 1972). *Cf. United States v. Bragan*, 499 F.2d 1376 (4 Cir. 1974).[19]

[19] The three reasons set forth in this paragraph also apply to Mr. Ewing's actions of December 30. *See* n. 16, *supra*.

The last of the objections raised in the court below to the evidence secured by the Milten Spy and the telephone traces was that it was detected and obtained in contravention of the Fourth Amendment. The district judge rejected this contention on the ground that even though the "spy" and the traces were utilized without prior judicial authorization, the evidence was obtained by searches to which the appropriate persons had consented, we need not review the soundness of that ruling or the implicit conclusions that the "spy" and the traces raised questions under the Fourth Amendment,[20] since in our opinion the activities complained of were, at most, conducted by private persons — OSI and the telephone company — to which the constitutional prohibition against warrantless searches does not apply. "[I]t is no part of the policy underlying the Fourth and Fourteenth Amendments to discourage citizens from aiding to the utmost of their ability in the apprehension of criminals," and consequently the Fourth

[20]Interceptions of two-party conversations were discussed in the context of the Fourth Amendment in the cases cited by the district court to support its conclusion. In each instance, government law enforcement officers had arranged and actively participated in the challenged surveillance. *See United States v. White*, 401 U.S. 745 (1971); *United States v. Bernstein*, 509 F.2d 996 (4 Cir. 1975); *United States v. Dowdy*, 479 F.2d 213 (4 Cir. 1973). *White* and *Dowdy* do support the view that the voluntary participation in such surveillance by one of the parties to a telephone call will satisfy the Fourth Amendment, and as already indicated, we tend to agree that even if Seidlitz's data transmissions were made with a legitimate expectation of privacy (a question we do not decide and about which we have serious reservations), the fact that OSI voluntarily recorded them obviates Fourth Amendment concerns as to the "spy". But we are not sure that a similar approach is valid with respect to the traces of the telephone numbers, and the parties have not briefed this aspect of the constitutional issue. Rather than decide either the "open" question of whether the Fourth Amendment applies to such traces, *see United States v. New York Tel. Co., supra*, 434 U.S. at 165 n. 7, or the more perplexing question of whether the recipient of a call can, under the Fourth Amendment, consent to a warrantless trace of the caller's telephone, we choose to rest our opinion as to the constitutionality of the "spy" and the traces on the ground set forth in the text.

Amendment and the exclusionary rule by which it is enforced come into play only where it appears from all of the circumstances that in a particular case the challenged evidence was obtained as a result of a search conducted by government officers or by private persons acting as agents or instrumentalities of the government. *Coolidge v. New Hampshire*, 403 U.S. 443, 487-490 (1971). *See also Burdeau v. McDowell*, 256 U.S. 465, 475-476 (1921); *United States v. Mekjian*, 505 F.2d 1320 (5 Cir. 1975); *United States v. Pryba*, 502 F.2d 391 (D.C. Cir. 1974), *cert. denied*, 419 U.S. 1127 (1975); *Corngold v. United States*, 367 F.2d 1 (9 Cir. 1966) (*en banc*). *Cf. United States v. Crabtree*, 545 F.2d 884 (4 Cir. 1976). Emphasizing that FEA's Mr. Coakley, upon discovering the suspicious initials, asked OSI's Ewing "if there was some way that he could determine what this account was doing,"[21] and that he asked OSI's Wack "if he could determine where the call was coming from,"[22] the defendant would have us find that the subsequent determination by OSI that the intruder was receiving the WYLBUR source code, as well as the telephone company's identification of the originating phone numbers, were actions for which the government should be held accountable and to which the Fourth Amendment applies. In our opinion, however, these nonspecific, innocuous remarks by a civilian employee of the FEA were in stark contrast to the active involvement by a Secret Service agent which tainted the search in *Lustig v. United States*, 338 U.S. 74 (1949), cited by the defendant,[23] and they do not amount to the

[21]Appendix, p. 41.

[22]Appendix, p. 42.

[23]*Lustig* presented the related question of whether, under the now defunct "silver platter" doctrine, a federal officer was so involved in an illegal search by city police as to require the suppression in a federal prosecution of the evidence uncovered by the search. The facts reveal that a federal Secret Service agent, who was charged with enforcing the counterfeiting laws, joined the unlawful search of a hotel room by city police after it had already begun. While there, he sifted through the

kind of conduct on the part of the government which has been held sufficient to deprive a citizen's search of its private character.[24] Under the criteria uniformly considered by the courts in assessing the degree of federal involvement in an otherwise private search for purposes of the Fourth Amendment, the instant "searches" and their fruits are not subject to scrutiny under the exclusionary rule.[25]

While we base our affirmance of the denial of the suppression motion upon our consideration of the statutory and constitutional arguments advanced by the appellant, and addressed by the court below, we think it appropriate to observe that we discern a certain speciousness which infects all of the illegal surveillance contentions made by the defendant with respect to the evidence which was obtained through use of the Milten Spy. Unlike the typical telephone user who employes the telephone merely as a convenience to converse with other persons over distances, Seidlitz used the telephone to tamper with and manipulate a machine which was owned by others, located on their premises, and

---

items uncovered by the local officers (who were aware of his interest in the case), selecting those articles which were later used as evidence in a federal counterfeiting prosecution of one of the occupants of the room. The Court found that the agent "had an active hand" in the search, and held that the trial court should have suppressed the evidence obtained by him.

[24] *See* the cases collected in *Annot.*, 36 A.L.R. 3d 553 (1971).

[25] The test most frequently employed is borrowed from the *Lustig* case, *supra*, 338 U.S. at 79, which recognized that "the decisive factor * * * is the actuality of a share by a federal official in the total enterprise of securing and selecting evidence by other than sanctioned means." *See also, United States v. Sherwin*, 539 F.2d 1, 7-8 (9 Cir. 1976); *United States v. Entringer*, 532 F.2d 634, 637 (8 Cir. 1976), *cert. denied*, 429 U.S. 820 (1976); *United States v. Clegg*, 509 F.2d 605, 609-611 (5 Cir. 1975); *United States v. Cangiano*, 464 F.2d 320, 324-325 (2 Cir. 1972), *vacated and remanded on other grounds*, 413 U.S. 913 (1973), *on remand*, 491 F.2d 905 (1973), *cert. denied*, 418 U.S. 934 (1973); *United States v. Johnson*, 451 F.2d 1321, 1322 (4 Cir. 1971), *cert. denied*, 405 U.S. 1018 (1972).

obviously not intended for his use. Unlike the party to a personal telephone call who may have little reason to suspect that his words are being covertly recorded, Seidlitz, a computer expert, undoubtedly was aware that by their very nature the computers would record the data he sent and received, and that OSI, also expert in the use of computers, could detect such exchanges if alerted to the presence of an intruder. In this sense the use by the witnesses below of the term "intruder" to describe an unauthorized user of the computers is aptly applied to the defendant, since by telephonic signal he in fact intruded or trespassed upon the physical property of OSI as effectively as if he had broken into the Rockville facility and instructed the computers from one of the terminals directly wired to the machines. Under these circumstances, having been "caught with his hand in the cookie jar", we seriously doubt that he is entitled to raise either statutory or constitutional objections to the evidence.

We have carefully reviewed the other issues raised by the appellant and find them to be without merit. Viewed in the light most favorable to the government, *Glasser v. United States*, 315 U.S. 60 (1942), there was sufficient evidence from which the jury could find that the WYLBUR system was "property" as defined in the instruction given by the trial judge which is not contested on appeal. Even though software systems similar to OSI's WYLBUR were in use at non-OSI facilities, the evidence that OSI invested substantial sums to modify the system to suit its peculiar needs, that OSI enjoyed a multi-million dollar competitive advantage because of WYLBUR, and that OSI took steps to prevent persons other than clients and employees from using the system permitted a finding that the pilfered data was the property of OSI and not, as the defendant contends, property in the public domain subject to appropriation by persons such as himself. In a similar vein, the defendant disputes the sufficiency of the evidence to establish fraudulent intent, but in essence his argument is

only that he feels the jury should not have discredited his own explanation of the purpose for which he acquired the WYLBUR data. It is of no consequence that Seidlitz was not shown by the government to have used the data retrieved from the OSI computers in his own business or to have attempted to sell it to others, *see United States v. Painter*, 314 F.2d 939 (4 Cir. 1963), *cert. denied*, 374 U.S. 831 (1963); *United States v. Bagdasian*, 291 F.2d 163 (4 Cir. 1961), *cert. denied*, 368 U.S. 834 (1961), and the circumstantial evidence in this case is ample to support a finding of the requisite intent.

On appeal, the defendant raises other objections relative to the searches of his office and residence, but these points were neither fairly raised in the motion to suppress evidence nor urged upon the trial court at the suppression hearing. Absent plain or fundamental error, we need not consider on appeal legal points which were available to the appellant but not presented for the district court's consideration. *United States v. Braunig*, 553 F.2d 777, 780 (2 Cir. 1977), *cert. denied*, 431 U.S. 959 (1977); *United States v. Rollins*, 522 F.2d 160, 165-166 (2 Cir. 1975), *cert. denied*, 424 U.S. 918 (1976); *United States v. Anderson*, 481 F.2d 685, 694-695 (4 Cir. 1973), *aff'd*, 417 U.S. 211 (1974). *See* Rules 12 (f) and 52, Federal Rules of Criminal Procedure.

AFFIRMED.

No. 78-1228

In the Supreme Court of the United States

OCTOBER TERM, 1978

BERTRAM E. SEIDLITZ, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

WADE H. McCREE, JR.
Solicitor General

PHILIP B. HEYMANN
Assistant Attorney General

KATHLEEN A. FELTON
Attorney
Department of Justice
Washington, D.C. 20530

In the Supreme Court of the United States

OCTOBER TERM, 1978

No. 78-1228

BERTRAM E. SEIDLITZ, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

OPINION BELOW

The opinion of the court of appeals is reported at 589 F. 2d 152.

JURISDICTION

The judgment of the court of appeals (Pet. App. A1-A16) was entered on December 5, 1978. A petition for rehearing was denied on January 9, 1979. The petition for a writ of certiorari was filed on February 7, 1979. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

QUESTIONS PRESENTED

1. Whether the Fourth Amendment's requirements apply to the tracing of telephone calls to determine their origin.

2. If so, whether the tracing in this case was a private search.

STATEMENT

Following a jury trial in the United States District Court for the District of Maryland, petitioner was convicted on two counts of wire fraud, in violation of 18 U.S.C. 1343. He was sentenced to three years' imprisonment on the first count, with all but three months suspended, and to three years' probation on the second count. The court of appeals affirmed (Pet. App. A1-A16).

In January 1975, petitioner became Deputy Project Director for Optimum Systems, Inc. (OSI), a private computer service company that was under contract to install, maintain, and operate a computer facility at Rockville, Maryland, for use by the Federal Energy Administration (FEA) (Tr. 3, 20, 24).[1] When completed, the computer facility was to be available to employees of FEA in various parts of the country through computer terminals in their offices, which could be connected with the central computer by ordinary telephone circuits (H. Tr. 40-41). As a security precaution, each authorized user of the computers was assigned a personal access code, which, when entered into the terminal and communicated to the central computers, would permit full use of the computers. As part of his broad responsibilities for the establishment and operation of the computer system, petitioner had full access to the computers and to a programming system contained in them, known as "WYLBUR," which had been specially modified by OSI for use by its clients (Tr. 13-20, 30-31). In June 1975, petitioner resigned from OSI and returned to work at his

[1] "Tr." refers to the trial transcript; "H. Tr." refers to the transcript of the hearing on petitioner's motion to suppress.

own computer firm in Alexandria, Virginia; his access code was deleted from the list of those identifying authorized users (Tr. 24, 26, 31, 153, 531).

On December 30, 1975, FEA and OSI employees discovered that an unauthorized person had gained access to the OSI computers (Tr. 75, 77). They determined that the computer was transmitting to the intruder a portion of the "source code" of the WYLBUR system[2] and that the data were being requested from outside the OSI facility, by a telephone connection (Tr. 131-134, 191). At the request of an OSI supervisor, the telephone company initiated a manual trace[3] to determine the origin of the call (H. Tr. 54-55). The telephone company informed OSI that the trace had been successful, but that the results of the trace could not be disclosed except in response to some legal action (H. Tr. 55). On the following day, when it appeared that the same intruder was again using the OSI computers, OSI again asked the telephone company to trace the call.

After December 31, OSI contacted the FBI (H. Tr. 56, 69, 78). Two more manual traces were conducted on January 5, at the suggestion of the FBI, but the calls were terminated before the traces had been completed (H. Tr. 67-69). Automatic equipment was then installed in the telephone company's Lanham, Maryland office, the last point to which the two previous calls had been traced, and on January 9, 1976, the equipment attributed two calls made to the OSI computers to a specific telephone

[2] A "source code" is the means used to give a computer instructions (Pet. App. A4 n.6).

[3] A manual trace involves a physical tracking of the telephone circuitry from the equipment that receives the call back through the various switching points to the equipment that originated the call. It is accomplished without listening to any conversation or intercepting any audible sounds (H. Tr. 64-66).

number in the area served by the Lanham office (H. Tr. 70-72).[4] The telephone company's trace records, which were obtained by the FBI pursuant to a subpoena, showed that the calls made on December 30 and 31 originated in petitioner's Virginia office, and that the calls on January 9 were made from petitioner's residence in Lanham, Maryland (H. Tr. 64-67, 71-73). Searches of petitioner's office and residence, both conducted pursuant to warrants, revealed a portable computer terminal, a copy of the user's guide to the OSI system as well as a notebook containing access codes for authorized users of the OSI computers, and some 40 rolls of computer paper on which were printed the WYLBUR source code (Tr. 247, 251, 258, 303-304, 311, 323).

ARGUMENT

1. Petitioner contends (Pet. 8-9) that his Fourth Amendment rights were violated by the use of special equipment to trace the telephone calls he made to the OSI computers. He claims that this case merits further review because the question whether a search warrant or court order is required for the use of a tracing device is identical to the issue presented in *Smith* v. *Maryland*, No. 78-5374, argued March 28, 1979.

In fact, however, the question to be decided in *Smith* v. *Maryland* is significantly different from the one petitioner poses. In *Smith*, the device at issue is a pen register,[5]

[4]The automatic equipment used by the telephone company operates like a manual trace, except that the automatic process is much faster. The equipment was programmed to record and print out any telephone number among that area's subscribers from which a call was placed to the OSI computers. Again, no audible sounds are intercepted in this process (H. Tr. 70).

[5]A pen register is a mechanical device that records the telephone numbers dialed from a monitored telephone. Its function is thus the reverse of a trace, which determines the origin of calls received by the monitored telephone. Neither device intercepts the content of a

which was installed on the defendant's telephone line when it was suspected that he was the person who had first robbed a woman and then made a series of obscene and threatening phone calls to her (*Smith* Pet. App. A2-A3). The question there is whether installation of the pen register without a warrant or court order was a violation of the defendant's Fourth Amendment rights.

While the operations of a pen register and a tracing device have similarities, there are significant differences in the nature of the privacy interests implicated because of the way the devices were used in the two cases. Thus, in *Smith* the petitioner claims a violation of his constitutionally protected privacy interests because *his* telephone was monitored by the pen register. In contrast, in the instant case, the monitored telephone belonged not to petitioner but to the recipient of his call, which had requested that its own phone be monitored in this fashion. Petitioner's claim here is accordingly only that he has a constitutionally protected privacy interest in making anonymous telephone calls. His interest is not substantially different from that of persons making obscene or threatening phone calls—such calls have traditionally been traced by the telephone company at the request of the victim or the police without any suggestion that the constitutional rights of the caller are being infringed. Cf. *United States* v. *Miller*, 425 U.S. 435, 443 (1976); *United States* v. *White*, 401 U.S. 745, 749 (1971); *Hoffa* v. *United States*, 385 U.S. 293, 302 (1966); *Lopez* v. *United States*, 373 U.S. 427 (1963).

We are of the view that the Fourth Amendment does not require either a warrant or probable cause as a prerequisite to the use of pen registers in official investigations. The pen register reveals only the number dialed, which is in substance a request to the telephone

communication. See *United States* v. *New York Telephone Co.*, 434 U.S. 159, 161 n.1 (1977); *Michigan Bell Tel. Co.* v. *United States*, 565 F. 2d 385, 388 n.5 (6th Cir. 1977).

company to complete a connection; it does not disclose whether the connection is made, still less the contents of the call. The telephone company's decision to disclose this information does not implicate personal privacy interests of sufficient significance to be considered a search within the scope of the Fourth Amendment. See *Hodge* v. *Mountain States Tel. & Tel. Co.*, 555 F. 2d 254, 256 (9th Cir. 1977); *United States* v. *Clegg*, 509 F. 2d 605, 610 (5th Cir. 1975).[6]

Even if this Court should conclude in *Smith* that the user of a monitored telephone has a privacy interest in the numbers he dials from the telephone substantial enough to merit the protection of a warrant or probable cause requirement, it does not follow that each person placing calls to a monitored telephone has a similarly substantial interest. As a result of a specific decision to focus on the caller's telephone, as in *Smith*, the entire pattern of the user's telephone communications is disclosed to the official investigation. In contrast, in the instant situation, there was no such specific focusing of the investigation on petitioner, and no similar surveillance of all the numbers he called. Instead, only two calls were identified as originating with his telephone. The privacy interest asserted by petitioner is at best analogous to those of the "casual visitor who walks into a house one minute before a search of the house commences and leaves one minute after the search ends"—interests that this Court in *Rakas* v. *Illinois*, No. 77-5781 (Dec. 5, 1978), slip op. 14, cited as an example of those not protected by the Fourth Amendment.[7]

[6]Alternatively, if the use of a pen register does involve a search, the substantial government interest in effective criminal investigations outweighs the limited intrusion into personal privacy involved in simply discovering the telephone numbers called, but not the contents of the calls. Cf. *Terry* v. *Ohio*, 392 U.S. 1, 21-25 (1968).

[7]Indeed, as the court of appeals noted (Pet. App. A14-A15), petitioner's position can also be analogized to an unauthorized intruder, since he "used the telephone to tamper with and manipulate

Finally, in the circumstances of this case petitioner's claim of a "reasonable expectation of privacy" is implausible. Petitioner was not conventionally using the telephone as a means of communicating; he was using it to evade a system that he well knew was designed to permit only carefully restricted access to the OSI computers. Petitioner cannot claim to have been an unsuspecting caller with little reason to believe that his calls might be traced. He must have expected that OSI would be alert to the possibility that unauthorized users might gain access to their computers and that it would make serious efforts to prevent such access and to identify those who attempted it. There is thus no basis for asserting a reasonable expectation of privacy with regard to the placing of these calls. See *United States* v. *White*, 401 U.S. 745, 749 (1971); *Katz* v. *United States*, 389 U.S. 347, 351-352 (1967).

2. Assuming *arguendo* that the Fourth Amendment would require the suppression of the fruits of an official investigation based on the warrantless tracing of OSI's telephone, the court of appeals correctly concluded that the discovery of petitioner's number here was the result of a private investigation by OSI and the telephone company (Pet. App. A12-A14).

Petitioner maintains that the installation of the tracing device was the result of governmental action, because the FBI had suggested that further tracing be attempted after the December 30 and 31 calls. In fact, however, the unsuccessful manual traces on January 5 and the use of

a machine which was owned by others, located on their premises, and obviously not intended for his use." It has been clear at least since *Jones* v. *United States*, 362 U.S. 257 (1960), that Fourth Amendment protections do not extend to one who is not legitimately on the premises searched. See *Rakas, supra*, slip op. 12-14.

Analytically, petitioner's argument would be the same if he were a burglar who had left fingerprints in his victim's house and was complaining about the warrantless entry of the police into that house, at the victim's request, to search for the fingerprints.

the automatic tracing equipment were part of a continuing effort to discover the identity of the unauthorized user of the computers, an effort undertaken and continued at the request of OSI. It was an OSI supervisor who first requested that the calls be traced on December 30 and 31; neither the local police nor the FBI were contacted until after those traces had been successfully completed. There is absolutely no indication that the initial traces were approved or participated in by any law enforcement officers, nor that the traces were requested by OSI for any reason other than their own desire to put a stop to the unauthorized use of their computer system. OSI's notification of and subsequent cooperation with the FBI is insufficient to convert an otherwise private search into government action subject to Fourth Amendment scrutiny. *Coolidge* v. *New Hampshire*, 403 U.S. 443, 448 (1971); *United States* v. *Lamar*, 545 F. 2d 488, 490 (5th Cir.), cert. denied, 430 U.S. 959 (1977); *United States* v. *Pryba*, 502 F. 2d 391, 401 (D.C. Cir. 1974), cert. denied, 419 U.S. 1127 (1975); *United States* v. *Blanton*, 479 F. 2d 327, 328 (5th Cir. 1973); *United States* v. *Harless*, 464 F. 2d 953, 956-957 (9th Cir. 1972); see also *Burdeau* v. *McDowell*, 256 U.S. 465, 475-477 (1921).[8]

---

[8]The cases cited by petitioner (Pet. 8) do not support his claim that federal officials had a "major share" in the telephone traces conducted in this case. In *United States* v. *Crabtree*, 545 F. 2d 884, 885-886 (4th Cir. 1976) (search of package by private air freight company), *United States* v. *Ford*, 525 F. 2d 1308, 1312 (10th Cir. 1975) (search of package by airline officials), and *United States* v. *West*, 453 F. 2d 1351, 1357 (3d Cir. 1972) (search of automobile by its owner at direction of police), the searches were held to have been conducted by private parties.

In *Corngold* v. *United States*, 367 F. 2d 1, 5-6 (9th Cir. 1966), customs agents had been following several men they suspected of smuggling watches and had already tested with radiation detection equipment some packages that had been consigned to an airline for shipping at the time they approached an airline employee and requested that the packages be opened. The court, in holding the search constituted federal action, relied on the fact that the search

The aim of the Fourth Amendment, and of the exclusionary rule fashioned to guarantee its observance, is to prevent official misconduct, not to discourage private citizens from aiding in the apprehension of criminals. *Coolidge* v. *New Hampshire, supra*, 403 U.S. at 488; *Burdeau* v. *McDowell, supra*, 256 U.S. at 475-476. Absent a valid claim of official instigation or participation in the search, petitioner can assert no Fourth Amendment protection.

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted.

WADE H. MCCREE, JR.
Solicitor General

PHILIP B. HEYMANN
Assistant Attorney General

KATHLEEN A. FELTON
Attorney

APRIL 1979

---

was conducted solely to further an ongoing federal investigation, as well as the fact that the customs agents actively joined in the search. Similarly, in *Smith* v. *Maryland, supra*, the pen register was installed, at police request, as part of a criminal investigation. Finally, in *Lustig* v. *United States*, 338 U.S. 74, 79 (1949), the "decisive factor" was that the federal official himself participated in the search of the premises.

DOJ-1979-04